Perancangan Kriptografi *Block Cipher 64 bit* Berbasis Pola *Launchpad*

The Chainsmokers - Closer (Launchpad Pro Cover) – YouTube

Artikel Ilmiah

Peneliti:
Korniawan Sorya Dinata KR (672013124)
Magdalena A. Ineke Pakereng, M.Kom.

Program Studi Teknik Informatika
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Salatiga
Mei 2017

PERPUSTAKAAN UNIVERSITAS
UNIVERSITAS KRISTEN SATYA WACANA
Jl. Diponegoro 52 – 60 Salatiga 50711
Jawa Tengah, Indonesia
Telp. 0298 – 321212, Fax. 0298 321433
Email: library@adm.uksw.edu ; http://library.uksw.edu

PERNYATAAN TIDAK PLAGIAT

Saya yang bertanda tangan di bawah ini:

Nama : KORNIAWAN SORYA DINATA KR

NIM : 672013124 Email : 672013124@student.uksw.edu

Fakultas : TEKNOLOGI INFORMASI Program Studi : TEKNIK INFORMATIKA

Judul tugas akhir : PERANCANGAN KRIPTOGRAFI BLOCK CIPHER 64 BIT BERBASIS POLA LAUNCHPAD THE CAMSMOKER - CLOSER (LAUNCHPAD PRO COVER) — YOUTUBE

Pembimbing : 1. Magdalena A. Ineke Pakereng, M.Kom.

2. _____

Dengan ini menyatakan bahwa:

1. Hasil karya yang saya serahkan ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar kesarjanaan baik di Universitas Kristen Satya Wacana maupun di institusi pendidikan lainnya.
2. Hasil karya saya ini bukan saduran/terjemahan melainkan merupakan gagasan, rumusan, dan hasil pelaksanaan penelitian/implementasi saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing akademik dan narasumber penelitian.
3. Hasil karya saya ini merupakan hasil revisi terakhir setelah diujikan yang telah diketahui dan disetujui oleh pembimbing.
4. Dalam karya saya ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali yang digunakan sebagai acuan dalam naskah dengan menyebutkan nama pengarang dan dicantumkan dalam daftar pustaka.

Pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari terbukti ada penyimpangan dan ketidakbenaran dalam pernyataan ini maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya saya ini, serta sanksi lain yang sesuai dengan ketentuan yang berlaku di Universitas Kristen Satya Wacana.

Salatiga, 15 JUNI 2017

Rp.6.000,-

KORNIAWAN SORYA DINATA KR

Tanda tangan & nama terang mahasiswa

F-LIB-080

PERPUSTAKAAN UNIVERSITAS
UNIVERSITAS KRISTEN SATYA WACANA
Jl. Diponegoro 52 – 60 Salatiga 50711
Jawa Tengah, Indonesia
Telp. 0298 – 321212, Fax. 0298 321433
Email: library@adm.uksw.edu ; http://library.uksw.edu

PERNYATAAN PERSETUJUAN AKSES

Saya yang bertanda tangan di bawah ini:

Nama : KORNIAWAN SORYA DINATA KR
NIM : 672013124 Email : 672013124@student.uksw.edu
Fakultas : TEKNOLOGI INFORMASI Program Studi : TEKNIK INFORMATIKA
Judul tugas akhir : PERANCANGAN KRIPTOGRAFI BLOCK CIPHER 64 BIT BERBASIS POLA LAUNCHPAD THE CHAINSMOKERS - CLOSER (LAUNCHPAD PRO COVER) - YOUTUBE

Dengan ini saya menyerahkan hak *non-eksklusif** kepada Perpustakaan Universitas – Universitas Kristen Satya Wacana untuk menyimpan, mengatur akses serta melakukan pengelolaan terhadap karya saya ini dengan mengacu pada ketentuan akses tugas akhir elektronik sebagai berikut (beri tanda pada kotak yang sesuai):

☑ a. Saya mengijinkan karya tersebut diunggah ke dalam aplikasi Repositori Perpustakaan Universitas, dan/atau portal GARUDA

☐ b. Saya tidak mengijinkan karya tersebut diunggah ke dalam aplikasi Repositori Perpustakaan Universitas, dan/atau portal GARUDA**

* *Hak yang tidak terbatas hanya bagi satu pihak saja. Pengajar, peneliti, dan mahasiswa yang menyerahkan hak non-eksklusif kepada Repositori Perpustakaan Universitas saat mengumpulkan hasil karya mereka masih memiliki hak copyright atas karya tersebut.*

** *Hanya akan menampilkan halaman judul dan abstrak. Pilihan ini harus dilampiri dengan penjelasan/ alasan tertulis dari pembimbing TA dan diketahui oleh pimpinan fakultas (dekan/kaprodi).*

Demikian pernyataan ini saya buat dengan sebenarnya.

Salatiga, 15 JUNI 2017

KORNIAWAN SORYA DINATA KR
Tanda tangan & nama terang mahasiswa

Mengetahui,

Magdalena A. Ineke Pakereng, M.Kom.
Tanda tangan & nama terang pembimbing I

Tanda tangan & nama terang pembimbing II

F-LIB-081

FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN SATYA WACANA
Jalan Diponegoro 52 – 60
Phone. (0298) 321212 (Hunting)
Fax. (0298) 321433
E-mail: fti@uksw.edu
Salatiga 50711 – INDONESIA

LEMBAR PERSETUJUAN PUBLISH JURNAL

Dengan mempertimbangkan isi dari jurnal mahasiswa :

Nama Mahasiswa : Kurniawan Soraya Dinata KR
NIM : 672013124

Maka jurnal ini dinyatakan :

LAYAK TERBIT / ~~**TIDAK LAYAK TERBIT**~~

Menyetujui,

Magdalena Ariutha Pakereng

Pembimbing 1

Pembimbing 2

Mengetahui,

Prof. Dr. Ir. Elko Sediyono, M.Kom

Reviewer

Lembar Pengesahan

Judul Artikel	: Perancangan Kriptografi *Block Cipher 64 byte* Berbasis Pola *Launchpad The Chainsmokes – Closer (Launchpad Pro Cover) - Youtube*
Nama Mahasiswa	: Korniawan Sorya Dinata KR
NIM	: 672013124
Program Studi	: Teknik Informatika
Fakultas	: Teknologi Informasi

Menyetujui,

Magdalena A. Ineke Pakereng, M.Kom.
Pembimbing

Mengesahkan

Dr. Dharmaputra T. Palekahelu, M.Pd	Dr. Kristoko Dwi Hartomo, M.Kom.
Dekan	Ketua Program Studi

Dinyatakan Lulus Tanggal : 18 Mei 2017

Reviewer :
2. Prof. Dr. Ir. Eko Sediyono, M.Kom. .....

Perancangan Kriptografi *Block Cipher 64 bit* Berbasis Pola *Launchpad*
The Chainsmokers - Closer (Launchpad Pro Cover) – YouTube

Artikel Ilmiah

Diajukan kepada
Fakultas Teknologi Informasi
untuk memperoleh Gelar Sarjana Komputer

Peneliti:
Korniawan Sorya Dinata KR (672013124)
Magdalena A. Ineke Pakereng, M.Kom.

Program Studi Teknik Informatika
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Salatiga

Mei 2017

1. Pendahuluan

Dalam rangka meminimalisasi celah Keamanan Data. Keamanan data pada komputer tidak hanya tergantung pada *firewall* dan *intrusion detection* system saja[1]. Berdasarkan hasil riset dan survei serta sebagian laporan tentang kejahatan komputer yang terjadi di dewasa ini, telah diketahui bahwa saat ini tidak ada satupun jaringan komputer yang dapat diasumsikan 100 persen aman dari serangan *virus, spam, e-mail, bomb* ataupun diterobos langsung oleh *hacker*. Satu hal yang perlu diingat adalah bahwa tidak ada satu system keamanan yang sempurna. Hal ini yang dapat lakukan hanyalah mencoba meminimalisasi celah keamanan yang ada pada komputer[2]. Hal ini peran utama kriptografi untuk mengamankan data atau dokumen dengan menggunakan teknik enkripsi, sehingga data dan dokumen tidak bisa dibaca[1].

Block cipher merupakan algoritma enkripsi kunci simetrik yang cara kerjanya per-blok, yaitu pada *bitstrings* yang panjangnya tetap [3]. Kebanyakan dari *block cipher* merupakan bagian dari *iterated block cipher* yang berarti blok dari *plaintext* diaplikasikan sebuah atau lebih transformasi sehingga menghasilkan *ciphertext* dengan panjang blok yang sama, dan proses tersebut diulang pada setiap *round* [4]. *Block cipher* memiliki dua algoritma yang berpasangan untuk masing-masing enkripsi dan dekripsi [5]. Dalam praktiknya, sebuah algoritma kriptografi akan mengenkripsi sebuah *plaintext* menjadi *ciphertext* berdasarkan kunci tertentu. Kriptografi yang digunakan dalam penelitian ini bersifat simetris yang merupakan metode enkripsi yang menggunakan kunci yang sama untuk enkripsi dan dekripsi. Algoritma Kriptografi terdiri dari tiga fungsi dasar yaitu *encripsi* yang diartikan dengan *chiper* atau kode, untuk merubah *plaintext* ke bentuk *ciphertext. Descripsi* merupakan kebalikan dari enkripsi, pesan yang telah dienkripsi dikembalikan ke bentuk asalnya *(Plaintext)*. Dan kunci yang di pakai untuk melakukan enkripsi dan deskripsi *(private key)* dan *(public key)*[1].

Algoritma pada perancangan kriptografi dalam penelitian ini adalah algoritma berbasis *Block Cipher* 64 bit dengan pola *launchpad the chainsmoker – closer (launchpad pro)-youtube.* Dari *launchpad* ini mempunyai keunikan pengacakan pola yang berubah-ubah mengikuti ritme lagunya. Menjelaskan bahwa semakin kompleks metode pengacakan yang digunakan maka akan semakin sulit untuk membongkar pesan yang terenkripsi ke bentuk aslinya dengan syarat kunci atau *private key* tidak boleh dipublikasikan kepada umum. Algoritma di kombinasikan dengan prinsip-prinsip kriptografi meliputi *tranposisi*, jaringan *fiestel* dan tabel substitusi *s-box* algoritma *AES (Advanced Encryption Standard*).

Dalam menjaga kerahasiaan data, kriptografi mentransformasikan data jelas *(plaintext)* ke dalam bentuk data sandi *(ciphertext)* yang tidak dapat dikenali. *Ciphertext* inilah yang kemudian dikirimkan oleh pengirim *(sender)* kepada penerima *(receiver)*. Setelah sampai di penerima, *ciphertext* tersebut ditranformasikan kembali ke dalam bentuk *plaintext* agar dapat dikenali[6]. Setiap blok berjumlah 64 bit, dan terdapat 24 putaran kombinasi dan 20 putaran enkripsi dan deskripsi dimana setiap putaran terdapat 4 proses.

2. Tinjauan Pustaka

Agar penelitian ini dapat di pertanggung jawabkan secara akademis, maka penelitian akan menampilkan penelitian yang telah dilakukan oleh penelitian terdahulu sebagai berikut:

Salah satunya dalam penelitian yang berjudul "Perancangan Algoritma Kriptografi Berbasis Pada Bagian Pohon" yang membahas tentang kriptografi *block cipher* dengan pola bagian pohon dari akar, batang daun hingga buahnya. Algoritma bagian pohon membuktikan bahwa pola ini dapat menghasilkan algoritma kriptografi simetris. Hasil dari perancangan algoritma kriptografi ini dapat digunakan untuk mengenkripsi dan mendekripsi teks yang kemudian mendapatkan hasil perbandingan nilai awal dan enkripsi[7].

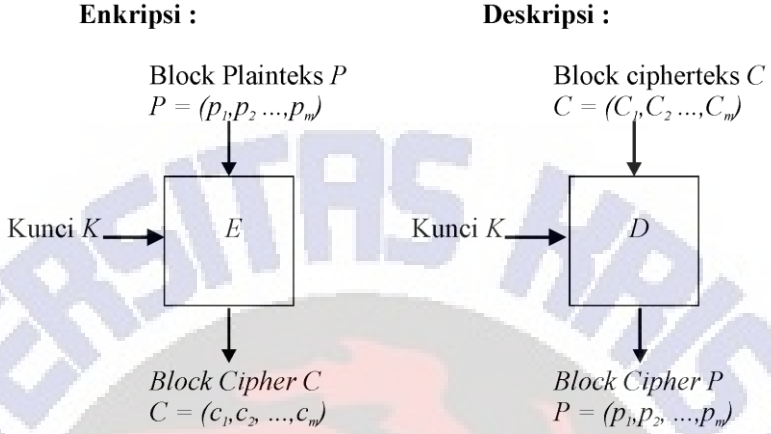
Penelitian kedua yang berjudul "Perancangan Kriptografi *Block Cipher* Berbasis Pola Ikan Berenang" yang membahas tentang algoritma yang di kembangkan berdasarkan prinsip *block cipher* dengan ukuran blok 64 bit. Hasil yang di peroleh dari penelitian ini bahwa pengguna proses *s-box, iterated cipher* dan jaringan *feistel* menghasilkan hasil rata–rata 43% dan korelasi dari 15 putaran menghasilkan nilai 0.21708[8].

Adapun penelitian ketiga berjudul "Pengaruh *s-box advanced encryption standard (AES)* Terhadap *avalanche effect* pada Perancangan Kriptografi *Block Cipher* 256 Bit Berbasis Pola Teknik Tarian Dansa Tali Dari Maluku" Dalam penelitian ini, perancangan kriptografi Berbasis Pola Teknik Tarian Dansa Tali memiliki 5 (lima) putaran proses enkripsi dimana hasil dari proses ke-2 dan ke-3 ditransformasi menggunakan tabel substitusi *S-Box*. Hasil yang di peroleh *Ciphertext* yang lebih acak pada pengujian *Avalanche Effect* yang sudah mencapai 50% sehingga dapat digunakan sebagai alternatif dalam pengamanan data[9].

Kriptografi adalah ilmu yang mempelajari bagaimana suatu pesan atau dokumen kita aman, tidak bisa dibaca oleh pihak yang tidak berhak. Dalam perkembangannya, kriptografi juga digunakan untuk identifikasi pengirim pesan dengan tanda tangan digital dan keaslian pesan dengan sidik jari digital *(fingerprint)*. Kriptografi mempunyai sejarah yang sangat panjang. Sejak jaman Romawi, Julius Caesar telah menggunakan teknik kriptografi yang sekarang dianggap kuno dan sangat mudah dibobol untuk keperluan komunikasi militernya. Namun sekutu dapat menembus Enigma, kriptografi produk Jerman dan Purple, kriptografi produk Jepang, sekutu akhirnya dapat memenangkan perang dunia kedua karena dapat mengetahui beberapa langkah dan strategi militer lawan[6].

Berdasarkan penelitian-penelitian yang pernah dilakukan terkait penerapan metode kriptografi tersebut menjadi acuan dalam membentuk ide untuk merancang penelitian baru maka akan dilakukan penelitian tentang Perancangan Kriptografi *Block Cipher 64 bit* Berbasis Pola Launchpad *The Chainsmokers - Closer (Launchpad Pro Cover) – YouTube.* Penelitian ini diharapkan dapat menghasilkan suatu teknik kriptografi baru. Pada penelitian ini sebelum proses enkripsi dilakukan dalam pencarian nilai korelasi terendah dari proses kombinasi 24 (dua puluh empat) putaran dengan memasukkan prinsip-prinsip kriptografi melipiti *tranposisi*, jaringan *fiestel* dan tabel substitusi *s-box* algoritma *AES (Advanced Encryption Standard*), setelah mendapatkan nilai kolerasi terendah

dilakupan proses enkripsi 20 (dua puluh) putaran. Mengkombinasikan *s-box* untuk mendapatkan avalance effect yang lebih baik dengan *ciphertext* yang lebih acak. Skema proses enkripsi dan dekripsi *block cipher* secara umum digambarkan pada Gambar 1.



Gambar 1 Skema enkripsi dan dekripsi pada *cipher* blok[10]

Misalkan blok *plaintext (P)* yang berukuran *m* bit dinyatakan sebagai vektor

$P = (p_1,p_2, ...,p_m)$ (1)

Yang dalam hal ini p_i adalah 0 atau 1 untuk i = 1,2, ..., m, dan *block ciphertext* (C) adalah

$C = (c_1,c_2, ...c_m)$ (2)

Yang dalam hal ini c_i adalah 0 atau 1 untuk i = 1,2, ..., m.

Bila *plaintext* dibagi menjadi *n* buah blok, barisan blok-blok *plaintext* dinyatakan sebagai

$(P_1,P_2, ..., P_n)$ (3)

Untuk setiap blok *plaintext* P_i, bit-bit penyusunnya dapat dinyatakan sebagai vektor

$Pi = (p_{i1},p_{i2}, ..., p_{im})$ (4)

Enkripsi dan deskripsi dengan kunci *K* dinyatakan berturut-turut dengan persamaan

$E_K(P) = C$ (5)

Untuk enkripsi, dan

$D_K(C) = P$ (6)

Fungsi *E* haruslah fungsi yang berkoresponden datu-ke-satu, sehingga

$E^{-1} = D$ (7)

Kunci (K) maka kunci adalah

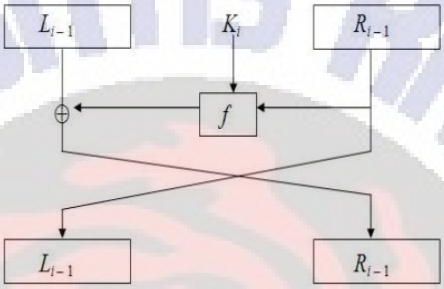
$K = (k_1,k_2, ..., k_n)$ (8)

Dalam penelitian kriptografi ini, terdapat beberapa prinsip yang digunakan antara lain. Prinsip-prinsip kriptografi meliputi *tranposisi*, jaringan *fiestel* dan tabel substitusi *s-box* algoritma *AES (Advanced Encryption Standard*). *Cipher* berulang *(iterated cipher)* merupakan blok *plaintext* yang mengalami pengulangan fungsi transformasi beberapa kali untuk mendapatkan blok *ciphertext*. Fungsi transformasi pada umumnya merupakan gabungan proses substitusi, permutasi,

kompresi, atau ekspansi terhadap blok *plaintext*. Sebuah kunci pada setiap putaran akan dikombinasikan dengan *plaintext*[8].

$$C\_i=f(C\_(i\text{-}l,)\ K\_i) \quad (9)$$

i = 1,2, …, r (r adalah jumlah putaran).
Ki = *Subkey* pada putaran ke-i.
f = Fungsi transformasi (didalamnya terdapat fungsi substitusi, permutasi, dan/atau ekspansi, kompresi).



Gambar 2 Skema Jaringan *Feistel* Pada *Block Cipher*[11]

Model yang dilakukan dalam jaringan Feistel adalah sebagai berikut:

1. Bagi blok yang panjangnya *n* bit menjadi dua bagian, kiri *(L)* dan kanan *(R)*, yang masing - masing panjangnya *n/2* (hal ini mensyaratkan *n* harus genap).
2. Definisikan cipher blok berulang dimana hasil dari putaran ke-i ditentukan dari hasil putaran sebelumnya (lihat Gambar 2), yaitu

$$L_i = R_i+1 \quad (10)$$
$$R_i = L_i - 1 \oplus f(R_i - 1, K_i) \quad (11)$$

i = 1, 2, …, r (r adalah jumlah putaran).
K_i = upa-kunci (subkey) pada putaran ke-i.
f = fungsi transformasi (di dalamnya terdapat fungsi substitusi, permutasi, dan/atau ekspansi,kompresi).

Avalanche Effect merupakan salah satu karakteristik untuk menentukan baik atau tidaknya suatu algoritma kriptografi. Suatu *avalanche effect* dikatakan baik jika perubahan bit yang dihasilkan berkisar antara 45-60% (sekitar separuhnya, 50% adalah hasil yang sangat baik).

$$Avalanche\ Effect = \frac{\sum bit\_berubah}{\sum bit\_total} \times 100\% \quad (12)$$

S-Box adalah matriks yang berisi substitusi sederhana yang memetakan satu atau lebih bit dengan satu atau lebih bit yang lain [11]. Pada kebanyakan algoritma *cipher blok*, *S-Box* memetakan m bit masukan menjadi *n* bit keluaran, sehingga *S-Box* tersebut dinamakan kotak *m* × *n S-box*. *S-box* merupakan satu-satunya langkah nirlanjar di dalam algoritma, karena operasinya adalah *look-up*

table. Masukan dari operasi *look-up table* dijadikan sebagai indeks *S-box*, dan keluarannya adalah *entry* di dalam *S-box*.

Dilanjutkan dengan pengujian statistika menggunakan kolerasi yang merupakan teknik statistik, yaitu suatu teknik statistik yang dipergunakan untuk mengukur kekuatan hubungan dua variabel dan juga untuk mengetahui bentuk hubungan antara dua variabel tersebut dengan hasil yang sifatnya kuantitatif. Kekuatan hubungan antara dua variabel biasanya disebut dengan koefisien korelasi dan dilambangkan dengan symbol "r". Nilai koefisien r akan selalu berada diantara -1 sampai +1. Untuk memudahkan menetukan kuat lemahnya hubungan antara variabel yang diuji maka dapat digunakan Tabel 1 [9].

Tabel 1 Klasifikasi Koefisien Korelasi.

Interval Koefisien	Tingkat Hubungan
0,00 – 0,199	Sangat Rendah
0,20 – 0,399	Rendah
0,40 – 0,599	Sedang
0,60 – 0,799	Kuat
0,80 – 1,000	Sangat Kuat

3. Metode dan Perancangan Algoritma

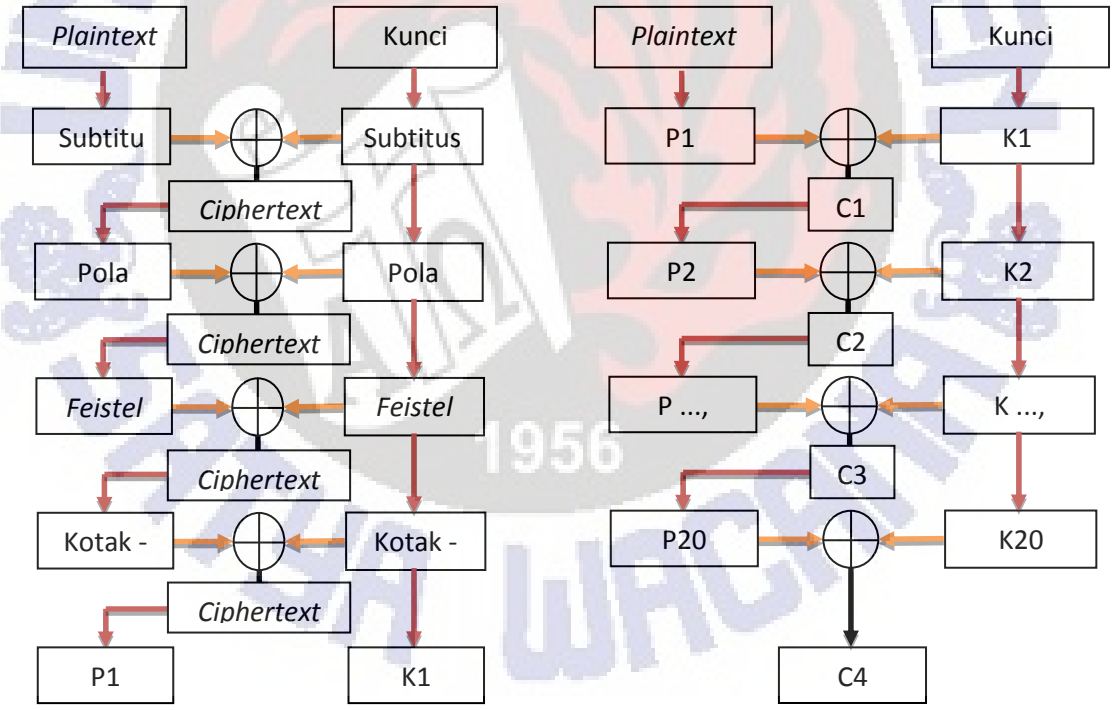
Penelitian yang dilakukan, diselesaikan melalui tahapan penelitian yang terbagi dalam lima tahapan, yaitu: (1) Analisis kebutuhan dan Identifikasi Masalah, (2) Pengumpulan Data dan Perancangan Sistem, (3) Implementasi dan Perancangan Kriptografi, (4) Pengujian Sistem, serta Analisis Hasil Pengujian, (5) Penulisan Laporan Hasil Penelitian.

Gambar 3 Tahapan Penelitian

Tahapan Penelitian pada Gambar 3 dapat dijelaskan sebagai berikut, *Tahap analisis kebutuhan dan identifikasi masalah* : Pada tahapan ini dilakukan analisis Terhadap permasalahan yang ada, terkait dengan proses perancangan Kriptografi berbasis *Launchpad; Tahap Pengumpulan Data dan Perancangan*

Sistem : Dalam tahapan ini dilakukan pengumpulan terhadap data dari jurnal-jurnal terkait, buku, serta sumber menengai pembahasan penelitian perancangan sistem tersebut; *Tahap Implementasi dan Perancangan Kriptografi :* Pada tahap ini akan dilakaukan perancangan Kriptografi berbasis pola *Launhcpad* untuk *plaintext* dan kunci yang di kombinasikan dengan XOR menggunakan proses enkripsi dan deskripsi yang di implementasikan pada *software excel* ; *Tahap Pengujian Sistem serta Analisa Hasil Pengujian :* Pada tahap ini dilakukan pengujian terhadap kriptografi yang telah dibuat. Pengujian melakukan pengacakan empat pola secara random dalam satu putaran yang di ulang sampai dua puluh putaran yang menghasilkan analisis korelasi; Apabila masih terjadi kesalahan maka perlu dilakukan perbaikan untuk mendapatkan hasil yang lebih baik. *Tahap Laporan Hasil Penelitian :* Dalam tahap terakhir ini dilakukan penulisan artikel tentang enkripsi dan deskripsi pada Perancangan Kriptografi *BlockChiper 64 bit* berbasisi pola *Launchpad*.

Dalam penelitian ini, perancangan algoritma kriptografi *Block Cipher* 64 bit berbasis pola *Launchpad*, dilakukan 4 (empat) proses untuk 1 (satu) putaran enkripsi. Enkripsi sendiri dilakukan dalam 20 putaran yang ditunjukan pada Gambar 4.



Gambar 4 Rancangan Alur Proses Enkripsi

Gambar 4 menggambarkan proses enkripsi, secara keseluruahan ada empat proses dalam satu putaran *plaintext* dan *kunci*. Yang menghasilkan empat *chipertext*. Langkah-langkah alur proses enkripsi dapat dijelaskan sebagai berikut: a) Menyiapkan *plaintext*; b) Mengubah *plaintext* menjadi biner sesuai dalam tabel ASCII; c) Dalam rancangan enkripsi *plaintext* dan kunci akan melewati empat proses pada setiap putaran yang dikombinasikan dengan prinsip-prinsip algoritma

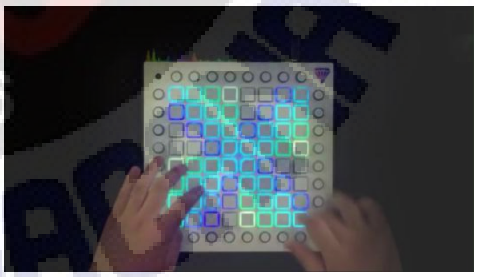
kriptografi: 1) Putaran pertama *Plaintext* 1 (P1) melakukan perumusan dengan pola *launchpad 1* dan di-XOR dengan Kunci 1 (K1) menghasilkan *Plaintext* 2 (P2); 2) *Plaintext* 2 (P2) melakukan perumusan dengan hasil dari proses pemasukan pola *launchpad 2* akan dilakukan proses disubstitusikan baris dan kolomnya dengan yang sudah ditentukan, kemudian di-XOR dengan Kunci yang sudah dilakukan proses substitusi baris dan kolomnya menghasilkan *Plaintext* 3 (P3); 3) *Plaintext* 3 (P3) melakukan perumusan dengan jaringan *feistel* dan di-XOR dengan Kunci yang juga telah dilakukan proses jaringan *feistel*; menghasilkan *Plaintext* 3 (P3); 3) *Plaintext* 3 (P3) melakukan perumusan dengan dilakukan proses *S-Box* dan di-XOR dengan Kunci yang juga telah dilakukan; 5) *Plaintext* 5 (P5) masuk pada putaran kedua dengan alur proses yang sama dengan putaran pertama, sampai berkelanjutan pada tahapan putaran ke-20 yang menghasilkan *Ciphertext (C).* Di lanjutkan ke proses deskripsi dengan alur proses yang sama sampai putaran ke-20 hingga menghasilkan *Ciphertext (C).*

4. Hasil dan Pembahasan

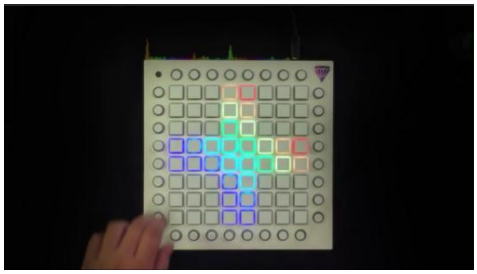
Di bagian ini akan membahas lebih terperinci mengenai algoritma perancangan kriptografi *block cipher* 64 bit dengan pola *launchpad the chainsmoker – closer (launchpad pro)-youtube.* Keuntungan menggunakan 64 bit adalah mampu menampung kapasistas memori lebih besar di banding 32 bit serta dalam penelitian ini menghasilkan perancangan algoritma kriptografi dengan pola baru. Membahas tentang proses enkripsi dan deskripsi, serta mengenai table substitusi untuk memperbesar analisis *avalanche effect.*

Dalam algoritma ini pola *launchpad the chainsmoker – closer (launchpad pro)-youtube.* Seni musik modern *launchpad* ini memiliki pola seperti yang digambarkan dalam Gambar 5.

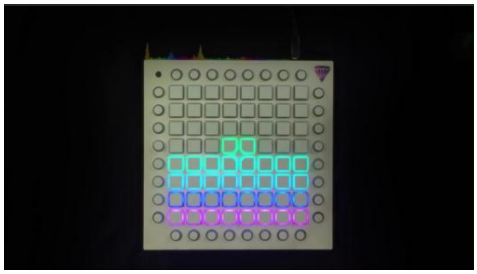
Pola (A)



Pola (B)



Pola (C)



Pola (D

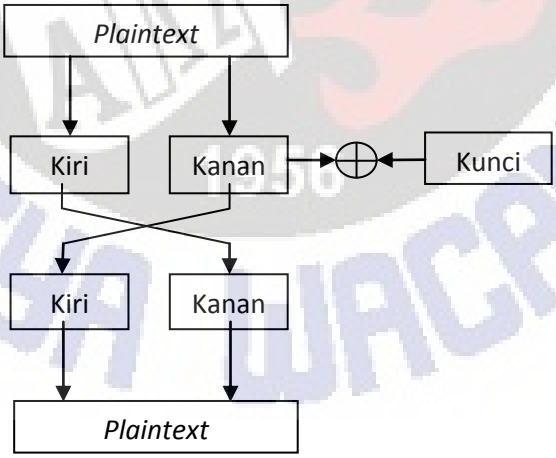
Gambar 5 Pola Teknik *launchpad the chainsmoker – closer (launchpad pro)-youtube*

Pada Gambar 5 terdapat 4 (empat) pola yang berbeda dimana pada pola-pola tersebut dapat dijelaskan bahwa di dalam seni musik *launchpad*, operator memainkan *launchpad* dengan memilih judul lagu *the chainsmoker – closer*. Kebetulan *launchpad* ini berbentuk kotak persegi yang di kelilingi tombol-tombol yang berjumlah 64 tombol dan di di bagian luar tombol setting *effect*. Operator memainkan *launchpad* dengan menekan tombol-tombol yang sudah di setting kemudian secara ritme lagu akan muncul bentuk pola-pola berwarna secara berurutan mengikuti ritme lagunya. Masing-masing pola berbeda untuk proses pengambilannya jadi proses pengambilan bit dimulai secara berurutan dari 1,2,3, ..., 64 sesuai masing-masing pola teknik.

Tabel 2 Proses Substitusi Kolom dan Baris[8]

Baris		Kolom	
1	8	1	5
2	7	2	4
3	2	3	7
4	1	4	3
5	4	5	6
6	3	6	1
7	6	7	8
8	5	8	2

Pada Tabel 2 merupakan salah satu prinsip-prinsip algoritma kriptografi untuk dilakukan rumus proses substitusi kolom dan baris di-*plaintext* dan di kunci dengan ketentuan pengacakan pada tabel di atas.



Gambar 6 Proses Jaringan *Feistel*

Pada Gambar 6 merupakan salah satu prinsip-prinsip algoritma kriptografi untuk dilakukan rumus proses jaringan *feistel*. Matrix 64-bit dibagi menjadi 2 (dua) kiri dan kanan. Pemprosessan dilakukan pada bagian bit kanan menjadi hasil di bagian kiri dan yang bit kiri awal nantinya menjadi kanan.

Berdasarkan pola-pola yang sudah dirancang, dilakukan pengujian korelasi atau nilai keterikatan antara *plaintext* dan *ciphertext* dengan

menkombinasikan urutan pola untuk mendapatkan rata-rata korelasi terbaik. Pengujian dilakukan dengan menggunakan 2 (dua) contoh *plaintext* yang berbeda yaitu :

- gbipUKSW
- GBIPuksw

Dengan menggunakan kunci : mAiP2472

Setelah mendapatkan hasil dari pengujian korelasi dengan contoh *plaintext* maka hasil rata-rata terbaik yang akan digunakan sebagai acuan perancangan dalam proses enkripsi.

Tabel 2 Tabel Rata Korelasi

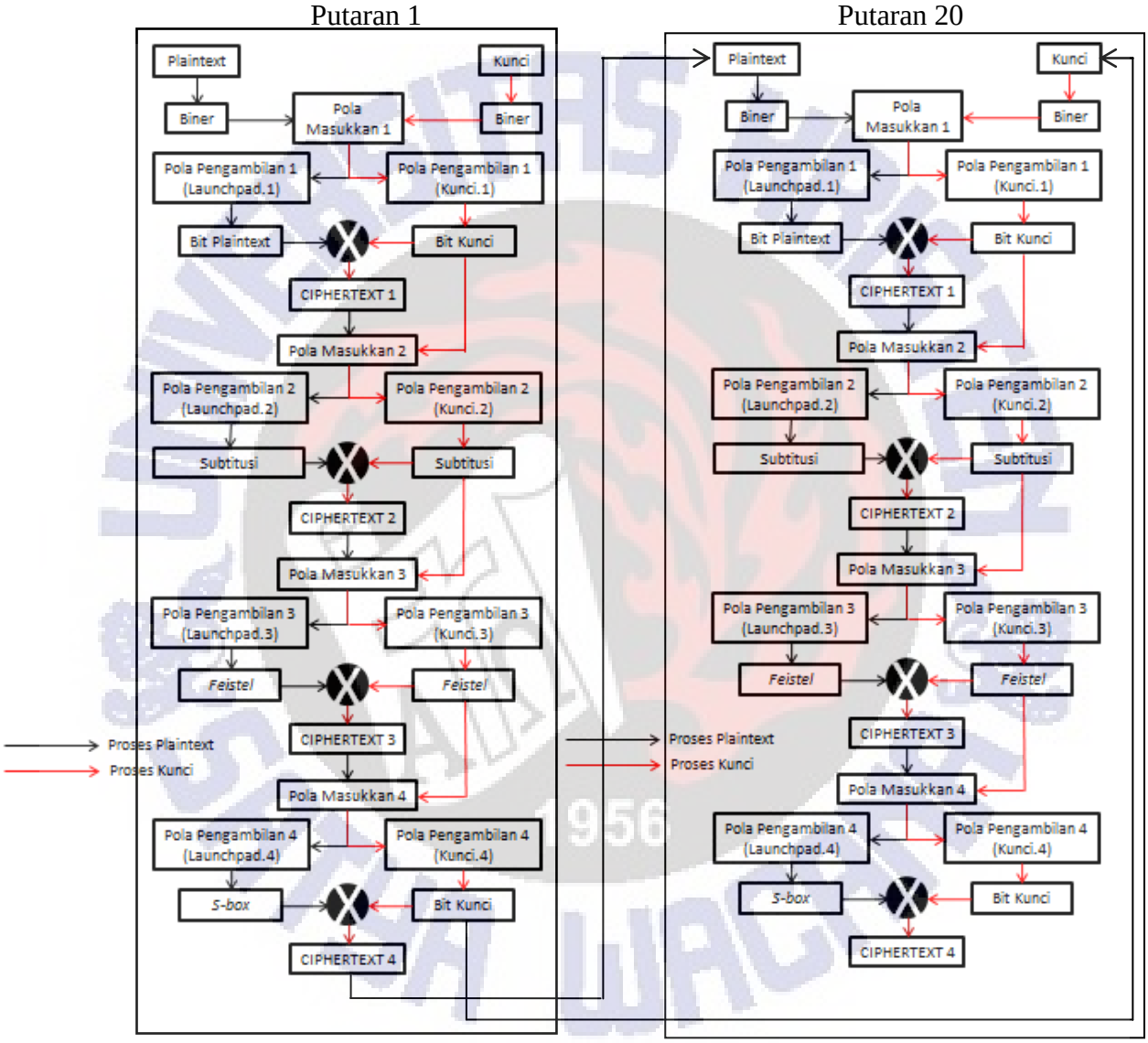
RATA-RATA NILAI KORELASI			
POLA	**RATA-RATA**	**POLA**	**RATA-RATA**
A-B-C-D	0,7170618	**C-A-B-D**	0,356361824
A-B-D-C	0,077158283	**C-A-D-B**	0,275779279
A-C-B-D	-0,572260676	**C-B-A-D**	0,301838504
A-C-D-B	0,29528921	**C-B-D-A**	-0,153745662
A-D-B-C	0,190381729	**C-D-A-B**	0,136440049
A-D-C-B	-0,05959212	**C-D-B-A**	0,282459791
B-A-C-D	-0,195579235	**D-A-B-C**	-0,150686918
B-A-D-C	0,574522821	**D-A-C-B**	0,393266753
B-C-A-D	-0,2415296	**D-B-A-C**	0,299867898
B-C-D-A	-0,451750654	**D-B-C-A**	-0,144578062
B-D-A-C	-0,497435806	**D-C-A-B**	-0,030708704
B-D-C-A	0,028384531	**D-C-B-A**	0,557324769

Tabel 2 menunjukkan bahwa urutan kombinasi pola dengan rata-rata korelasi terbaik terdapat pada urutan pola B-D-C-A. Kombinasi ini pun akan dilanjutkan proses enkripsinya sampai putaran ke-20 untuk menghasilkan *ciphertext.*

Sudah Di jelaskan sebelumnya bahwa pola *launchpad the chainsmoker – closer (launchpad pro)-youtube* 64 bit. Dilakukan sampai perputaran 20 (dua puluh) untuk mendapatkan *ciphertext* yang terbaik dan di setiap pitaran terdapat 4 (empat) proses yang di kombinasikan dengan prinsip-prinsip kriptografi. Secara rinci proses enkripsi dapat di lihat pada Gambar 7. Di awali dengan proses *plaintext* dan kunci dikonversi menjadi ASCII kemudian diubah ke bilangan biner. Hasil *plaintext* kemudian dimasukkan ke dalam kolom matrix 8 x 8 menggunakan pola pemasukkan yang sudah di tentukan dan di lanjutkan pengambilan dengan pola *launchpad* serta dalam satu putaran terdapat 4 (empat) proses prinsip-prinsip algoritma kriptografi. Proses pertama *plaintext* ditranformasikan dengan pola *launchpad* untuk menghasilkan C1, proses kedua *plaintext* dan kunci ditransformasikan dengan substitusi baris dan kolom untuk menghasilkan C2, proses ketiga *palintext* dan kunci ditransformasikan dengan jaringan *feistel* untuk mendapatkan hasil C3, proses keempat *plaintext* di tranformasikan dengan *s-box* untuk menghasilkan C4. Masuk pada putaran kedua

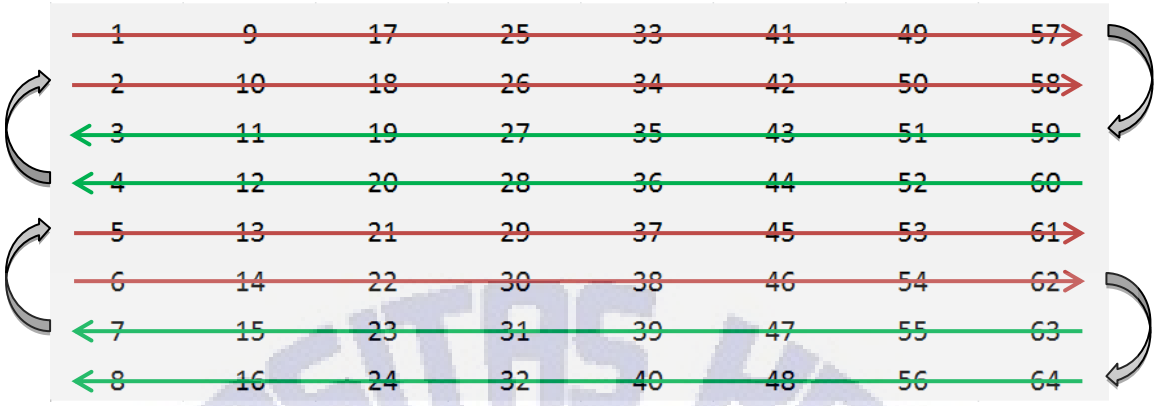
sama denga alur proses putaran pertama dengan proses pemasukkan bit proses putaran pertama, jadi C4 sama dengan P1 dan K4 sama dengan K1 pada putaran kedua. Di lanjutkan sampai dengan putaran ke-20.

- **Proses Enkripsi**



Gambar 7 Rancangan Alur Proses Enkripsi

Untuk menjelaskan secara rinci proses pemasukan bit dalam matriks 8 x 8 maka diambil proses 1 dan 2 pada putaran 1 sebagai contoh. Misalkan angka 1 merupakan inisialisasi setiap bit yang merupakan hasil konversi *plaintext* maka urutan bit adalah sebagai berikut 1, 2, 3, 4, ..., 64.



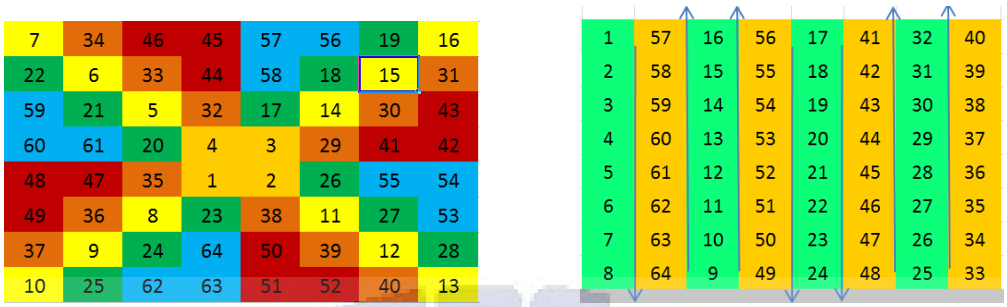
Gambar 8 Alur Proses Pemasukan Bit*Plaintext*

Gambar 5 menggambarkan proses pemasukan *plaintext* P1 sampai dengan P4 dan proses pemaskukan kunci yang akan diubah menjadi biner dan dimasukkan ke dalam matriks 64-bit. Di ambil dari table proses *plaintext* menjadi biner sesuai dalam tabel ASCII. Langkah pertama memasukkan bit secara horizontal dari table proses *plaintext* di mulai dari kolom pertama berlanjut mengulir dari atas ke bawah dan kembali ke atas dengan sesuai alur pemasukkan gambar di atas.

Pola 1 Kunci *(key)* 1

Gambar 9 Pola Teknik *launchpad the chainsmoker – closer (launchpad pro)-youtube*

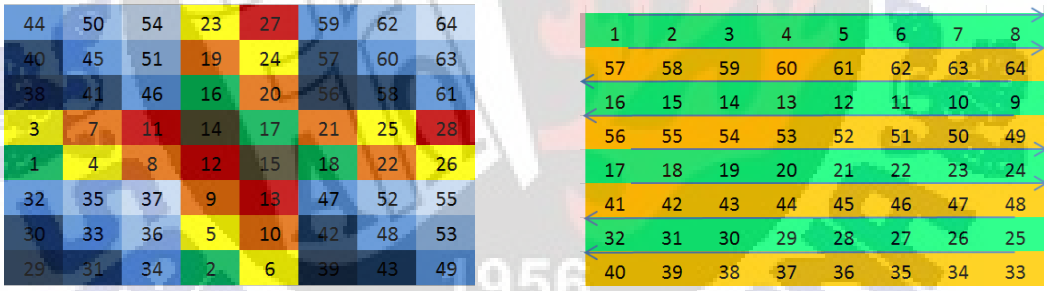
Gambar 9 merupakan proses pengambilan *plaintex*t dan kunci *(key)*. Bit diambil setiap 64 bit mengikuti urutan angka pada gambar dengan urutan gambar pola 1 yaitu dari tengah menyebar membentuk plus lalu membentuk silang dari dalam keluar dan mengakhiri dengan menutupi semua ruang yang belum di lalui. Gambar kunci *(key)* 1 di awali dengan horizontal dari atas ke bawah dan sebaliknya seperti ulir. Kemudian dimasukan ke dalam kolom matrixs 8 x 8 mengikuti anak panah dan urutan angka pada gambar. Hasil transposisi dari *plaintext* dan kunci *(key)* kemudian di-XOR sehingga menghasilkan *ciphertext* 1 yang kemudian digunakan sebagai P2 pada proses ke-2.



Pola 2 Kunci *(key)* 2

Gambar 10 Pola Teknik *launchpad the chainsmoker – closer (launchpad pro)-youtube*

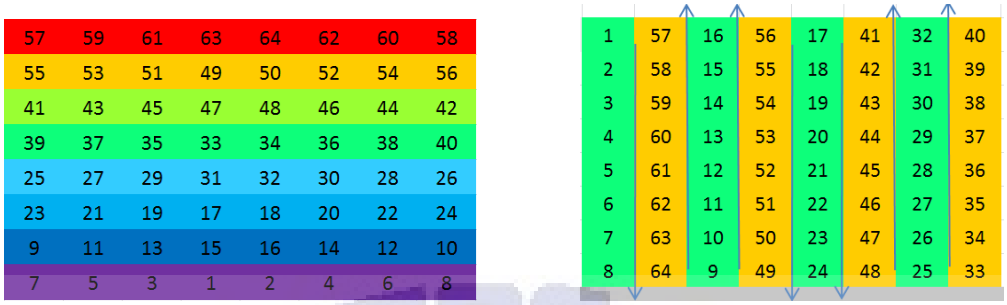
Gambar 10 merupakan proses pengambilan *plaintext* dan kunci *(key)*. Bit diambil setiap 64 bit mengikuti urutan angka pada gambar dengan urutan gambar pola 2 yaitu dari tengah menyebar membentuk silang lalu berjalan membentuk kipas berputar berlawanan arah jarum jam memenuhi kolom matrix. Gambar kunci *(key)* 2 di awali dengan vertikal dari kanan ke kiri dan sebaliknya seperti ulir. Kemudian dimasukkan ke dalam kolom matriks 8 x 8 mengikuti anak panah dan urutan angka pada gambar. Pada pola 2 di kombinasikan dengan proses trasnposisi baris dan kolom bit *plaintext* dan kunci *(key)*. Hasil transposisi dari *plaintext* dan kunci *(key)* kemudian di-XOR sehingga menghasilkan *ciphertext* 2 yang kemudian digunakan sebagai P3 pada proses ke-3.



Pola 3 Kunci *(key)* 3

Gambar 11 Pola Teknik *launchpad the chainsmoker – closer (launchpad pro)-youtube*

Gambar 11 merupakan proses pengambilan *plaintext* dan kunci *(key)*. Bit diambil setiap 64 bit mengikuti urutan angka pada gambar dengan urutan gambar pola 1 yaitu membentuk plus di awali dari pojok kiri bawah menyamping kanan ke atas lalu berjalan memenuhi kolom matrix seperti warna gradasi gambar pola 3. Gambar kunci *(key)* 3 di awali dengan horizontal dari atas ke bawah dan sebaliknya seperti ulir. Kemudian dimasukkan ke dalam kolom matriks 8 x 8 mengikuti anak panah dan urutan angka pada gambar. Pada pola 3 di kombinasikan dengan proses jaringan *feistel* bit *plaintext* dan kunci *(key)*. Hasil dari jaringan *feistel* bit *plaintext* dan kunci *(key)* kemudian di-XOR sehingga menghasilkan *ciphertext* 3 yang kemudian digunakan sebagai P4 pada proses ke-4.



Pola 4 Kunci *(key)* 4

Gambar 12 Pola Teknik *launchpad the chainsmoker – closer (launchpad pro)-youtube*

Gambar 12 merupakan proses pengambilan *plaintext* dan kunci *(key)*. Bit diambil setiap 64 bit mengikuti urutan angka pada gambar dengan urutan gambar pola 4 yaitu ada dua gerakan ulir dari tengah bawah ke atas berjalan berlawanan hingga berakhir di tengah atas memenuhi kolom matrix. Gambar kunci *(key)* 4 di awali dengan vertikal dari kanan ke kiri dan sebaliknya seperti ulir. Kemudian dimasukkan ke dalam kolom matriks 8 x 8 mengikuti anak panah dan urutan angka pada gambar. Pada pola 4 di kombinasikan dengan proses *s-box* pada table substitusi *s-box* bit *plaintext*. *Plaintext* 4 kemudian diambil setiap 8 bit sesuai dengan pola pemasukan menjadi biner. Hasil biner di ubah menjadi desimal kemudian di konversi kembali ke *hexa*. Kemudian *hexa* dikonversikan dengan table substitusi *s-box*.Hasil transposisi dari *plaintext* dan kunci *(key)* kemudian di-XOR sehingga menghasilkan *ciphertext* 4. S-Box sendiri berfungsi untuk Transformasi *SubBytes()* memetakan setiap *byte* dari array *state*.

Tabel 3 Tabel Substitusi *S-Box* AES

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	J0	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	DB	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	BE	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	OD	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Tabel 3 merupakan tabel kotak-s yang digunakan dalam proses substitusion box *(S-Box)* enkripsi. Cara pensubstitusian adalah sebagai berikut: untuk setiap *byte* pada array *state*, misalkan *S[r, c] = xy*, yang dalam hal ini *xy* adalah digit heksadesimal dari nilai *S[r, c]*, maka nilai substitusinya, dinyatakan dengan *S'[r, c]*, adalah elemen di dalam *S-box* yang merupakan perpotongan baris *x* dengan kolom *y*.Misalnya *S[0, 0] = 19*, maka *S'[0, 0] = d4*.

Untuk pengujian algoritma dilakukan dengan mengambil *plaintext* adalah gbipUKSW dan kunci adalah mAiP2472. Setelah melakukan proses enkripsi yang telah di jelaskan sebelumnya maka perancangan mendapatkan *ciphertext* yang telah di konversi ke dalam nilai *hexadecimal*.

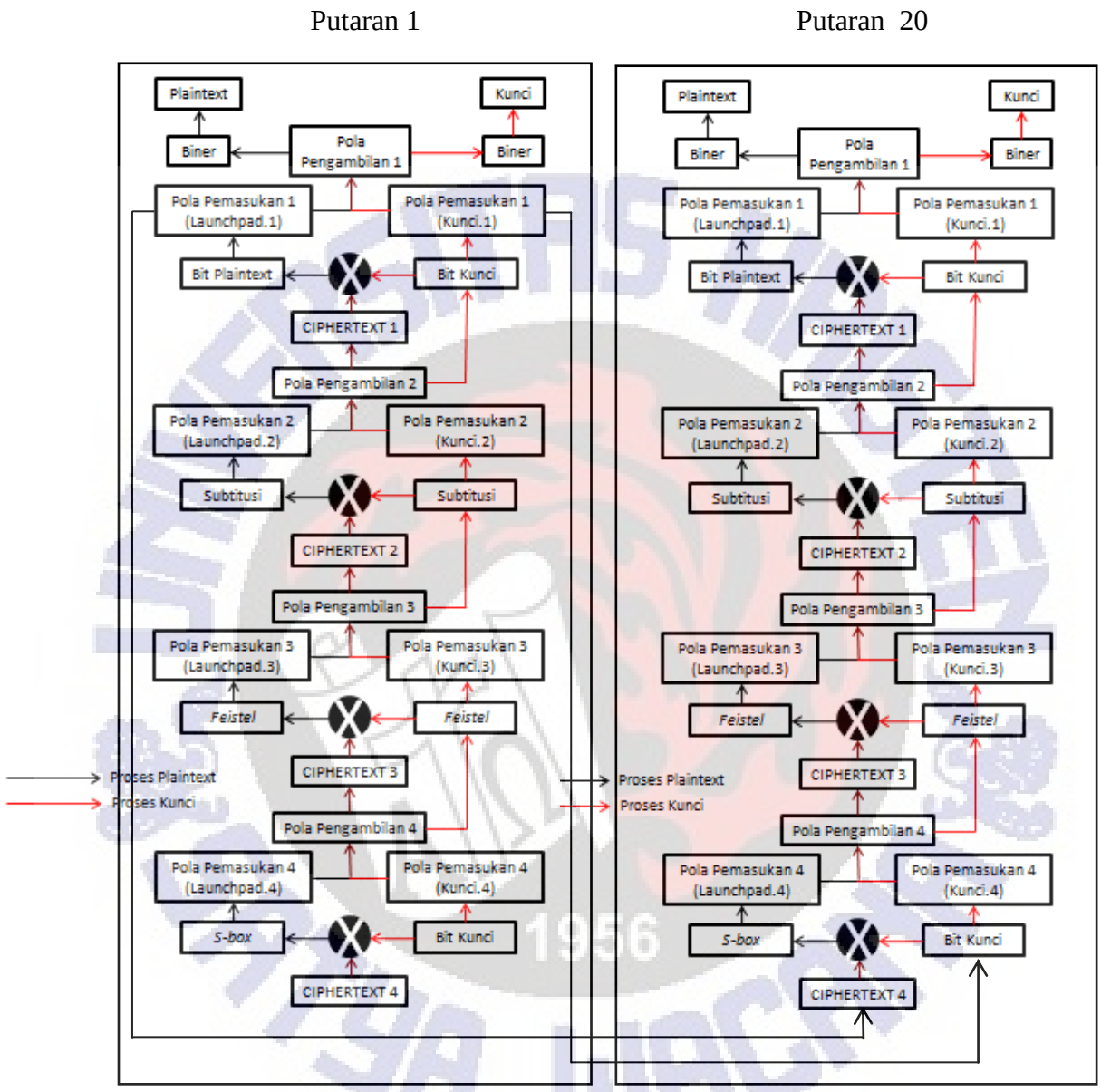
Tabel 4 Hasil enkripsi *Ciphertext* setiap putaran

HASIL CIPHERTEXT			
Putaran	***hexadecimal***	**Putaran**	***hexadecimal***
1	D025711E35BB9B8	**11**	C912FA83D8282777
2	CB1E3E173EFDA87A	**12**	247F71AFB99F8CA
3	4CFC197934F5DB6	**13**	31947AC4701312E8
4	D65DAEA680A88AA9	**14**	3E8812EB2877212
5	79DA5D66A26ABA	**15**	AC52222EF12E316F
6	42CE673DE276C6D7	**16**	BF2667F0959846E1
7	B6F6A13F3FA48BF	**17**	13D2431A20143993
8	135E1518F6C0A153	**18**	542DB85E46516
9	7DC565A2B3A468D8	**19**	4BCA9E02B7AC959
10	A9AE48F31898FBAE	**20**	B4225C8951CBFAC

Tabel 4 merupakan hasil enkripsi dari setiap putaran. Hasil dari 20 putaran yang mendapatkan *final ciphertext*.

Proses deskripsi merupakan kebalikan dari proses enkripsi. Deskripsi dilakukan dari P4 dan K4 yang di ambil dari hasil proses P4 dan K4 enkripsi putaran ke-20. P4 di-XOR dengan K4 sampai menghasilkan P1, berkelanjutan sampai deskripsi putaran ke-20.

- **Proses Deskripsi**



Gambar 13 Skema Proses Deskripsi

Gambar 13 menggambarkan alur proses pengambilan deskripsi, secara keseluruahan ada empat proses dalam satu putaran *plaintext* dan *kunci.* Yang menghasilkan empat *chipertext.* Pola pengambilan bit proses enkripsi pada proses deskripsi digunakan sebagai pola pemasukkan. Sebaliknya pola pemasukkan pada proses enkripsi akan digunakan sebagai pola pengambilan dekripsi sehingga pola *launchpad* di proses deskrip digunakan sebagai pola pemasukkan bit pada proses deskripsi.

Proses dekripsi dimulai dengan memasukkan *ciphertext* pada kolom matriks C4 kemudian di-XOR dengan K4 hasil proses kunci pada proses keempat.

Hasil XOR kemudian ditransposisikan menggunakan pola substitusi table *s-box*. *Plaintext* 4 kemudian diambil setiap 8 bit sesuai dengan pola pemasukan menjadi biner. Hasil biner di ubah menjadi desimal kemudian di konversi kembali ke *hexa*. Kemudian *hexa* dikonversikan dengan table substitusi *s-box*. Bit hasil substitusi *s-box* diambil menngunakan pola *launchpad* untuk mengisi kolom metrix P4 . Hasil dari *plaintext* dari P4 digunakan untuk C3 dan kunci *(key)* K4 digunakan untuk K3. Proses seterusnya sampai P1 dan K1 sama hingga menghasilkan *ciphertext* dan berkelanjutan sampai putaran ke-20.

Tabel 5 Algoritma Proses Enkripsi dan Dekripsi.

Algoritma Proses Enkripsi	Algoritma Proses Deskripsi
1. Masukkan *plaintext* dan Kunci *(key)* 2. *Plaintext* diubah ke ASCII 3. ASCII diubah ke BINER 4. Bit BINER dimasukan ke kolom P1 menggunakan pola masuk *Plaintext* 5. Bit P1 dimasukkan dengan pola *Launchpad 1* 6. P1 di-XOR dengan K1 menghasilkan C1 7. C1 = P2 8. Bit P2 di masukkan dengan pola *Launchpad 2*, hasilnya P2 dan K2 disubstitusikan baris dan kolom 9. P2 di-XOR dengan K2 menghasilkan C2 10. C2 = P3 11. Bit P3 BINNER dibagi 2 kanan dan kiri 12. Kanan disubstitusikan dengan K2 13. BINNER kiri dimasukkan ke kanan dan kiri dimasukkan ke kanan 14. P3 di-XOR dengan K3 menghasilakan C3 15. C3 = P4 16. Bit P4 dimasukkan dengan pola *Launchpad 4* 17. P4 diubah ke BINER 18. BINER diubah ke HEXA 19. HEXA dimasukkan ke S-BOX 20. Hasil HEXA invers diubah ke BINER 21. P4 di-XOR dengan K4 menghasilkan C4 22. C4 diubah ke BINER 23. BINER diubah ke ASCII 24. ASCII diubah ke HEXA	1. Masukkan C4 2. C4 diubah ke ASCII 3. ASCII diubah ke BINER 4. Bit BINER dimasukkan ke kolom matrix C4 menggunakan pola masuk *Plaintext* 5. Masukkan bit K4 menggunakan pola masukkan 6. C4 di-XOR dengan K4 7. Bit P4 diubah ke BINNER 8. BINNER diubah ke HEXA 9. HEXA dimasukkan ke dalam tabel *S-BOX* 10. Hasil HEXA invers diubah ke BINER 11. BINNER P4 dimasukkan ke kolom metrix dengan pola *launchpad 4* 12. P4 = C3 13. BINNER dimasukkan kedalam kolom C3 menggunakan pola masuk *plaintext* 14. C3 di-*XOR* dengan K3 15. Hasil XOR kolom metrix dibagi 2 kanan dan kiri 16. BINNER dibalik kiri menjadi kanan dan kanan menjadi kiri 17. BINNER kiri disubtitusikan dengan K2 18. P3 = C2 19. BINNER dimasukkan kedalam kolom C2 dimasukkna kedalam kolom menggunakan pola *plaintext* 20. C2 di-*XOR* dengan K2 21. Hasil XOR disubstitusikan terbalik baris dan kolom 22. P2 = P1 23. BINER dimasukkan kedalam kolom C1 menggunkan pola *plaintext* 24. C1 di-*XOR* dengan K1 25. Hasil XOR dimasukkan dengan pola *Launchpad 1* menghasilkan P1 26. P1 diubah ke BINER 27. BINER diubah ke ASCII 28. ASCII diubah ke CHAR

Tabel 5 merupakan algoritma proses enkripsi dan dekripsi. Proses enkripsi menghasilkan C4 sedangkan proses dekripsi menghasilkan P1.

Algoritma proses Kunci *(Key)*,dijelaskan sebagai berikut:

1. Masukkan Kunci
2. Kunci diubah ke ASCII
3. ASCII diubah ke BINER
4. Bit BINER dimasukan ke kolom K1 menggunakan pola masuk Kunci
5. Bit Kunci ditransposisikan dengan pola Kunci A
6. Transposisi K1 = K2
7. K2 ditransposisikan menggunakan pola Kunci B
8. K2 = K3
9. K3 ditransposisikan menggunakan pola Kunci C
10. K3 = K4
11. K4 ditransposisikan menggunakan pola Kunci D

Pseudocode proses enkripsi dan dekripsi dijelaskan sebagai berikut :

Proses Enkripsi
{Program ini digunakan untuk melakukan proses enkripsi data}

Kamus
P,K,P1,P2,P3,P4,K1,K2,K3,K4,A,B = integer
C1,C2,C3,C4 = integer

```
Start
        C1 <- P1 ⊕ K1
                Input P
                Read P
                        P to ASCII
                        ASCII to BINER
                        Dari BINER = kolom metrixs P1, masukan BINER
                                P1 Transposisi  menggunakan pola Launchpad 1
                Output P1

                Input K
                Read K
                        K to ASCII
                        ASCII to BINER
                        Dari BINER = kolom matrrixs K1,masukan BINER
                                K1 Transposisi menggunakan Kunci A
                Output K1
        Print C1
        C1 = P2
        C2 <- P2 ⊕ K2
                C1 = kolom matrixs P2, masukan C1
                        P2 substitusi baris dan kolom
                Output P2
                K1 = kolom matrixs K2, masukan K1
                        K2 substitusi baris dan kolom
                Output K2
        Print C2
        C2 = P3
        C3<- P3⊕ K3
                C2 = kolom matrixs P3, masukan C2
                        P3 bit dibagi 2 -> A,B
                Output P3
                K2 = kolom matrixs K3, masukan K2
                        K3 bit dibagi 2 -> A,B
                Output K3
                B = B ⊕ K2
```

```
                P3 = B ,A
        Print C3
        C3 = P4
        Biner S-Box<- Invers Hexa C3
                C3 to BINER
                BINER to HEXA
                Dari HEXA =  Tabel S-Box, masukan HEXA
                HEXA Substitusi menggunakan S-Box
        Print BINER S-Box
        C4 <- P4⊕ K4
                Dari BINER S-Box = kolom matrixs P4, Masukan BINER S-Box P4
                Output P4
                Dari K3 = kolom matrixs K4, Masukan BINER S-Box K4
                Output K4
        Print C4
Repeat

End
```

Proses Deskripsi

{Program ini digunakan untuk melakukan deskripsi data}

```
Kamus
P,C,K,P1,P2,P3,P4,K1,K2,K3,K4,A,B = integer
C1,C2,C3,C4 = integer

Start
        K4
                Input K
                Read K
                        K4 Transposisi menggunakan pola masukan kunci D
        Output K4

        K3 <- Transposisi K4
                K3 bit dibagi 2 -> A,B
        Output K3

        K2<- Transposisi  K3
                K2 substitusi baris dan kolom
        Output K2

        K1 <- Transposisi  K2
                K1 Transposisi menggunakan  pola masukan Kunci A
        Output K1

        P4 <- C4⊕ K4
                Input C
                Read C
                        C4 to ASCII
                        ASCII to BINER
                        BINER to HEXA
                        Dari HEXA =  Tabel  S-Box, masukan HEXA
                        HEXA Substitusi menggunakan S-Box
                        C4⊕ K4
        Print P4

        P3 <- C3⊕ K3
                P3 bit dibagi 2 -> A,B
                C3⊕ K3
        Print P3

        P2 <- Transposisi dari hasil C3⊕ K3
                P2 substitusi baris dan kolom
        Print P2
        P2=C1

        P1<- Transposisi dari hasil C1⊕ K1
                P2 ⊕ K2
                Transposisi menggunakan pola Launchpad 1
        Print P1
```

P1 to BINER
BINER to ASCII
ASCII to CHAR
Print P

End

Pengujian AE*(Avalanche effect)* digunakan untuk mengukur seberapa acak perbandingan antara hasil enkripsi (*ciphertext*) dan *plaintext.*

Tabel 6 Hasil Uji AE pada GPCK

PUTARAN	BANYAK BIT BERUBAH	*AVALANCHE EFFECT*
1	22	34,375
2	40	62,5
3	38	59,375
4	32	50
5	37	57,8125
6	25	39,0625
7	39	60,9375
8	31	48,4375
9	34	53,125
10	27	42,1875
11	26	40,625
12	32	50
13	30	46,875
14	34	53,125
15	30	46,875
16	30	46,875
17	33	51,5625
18	33	51,5625
19	31	48,4375
20	30	46,875
	Rata-rata	49,53125 %

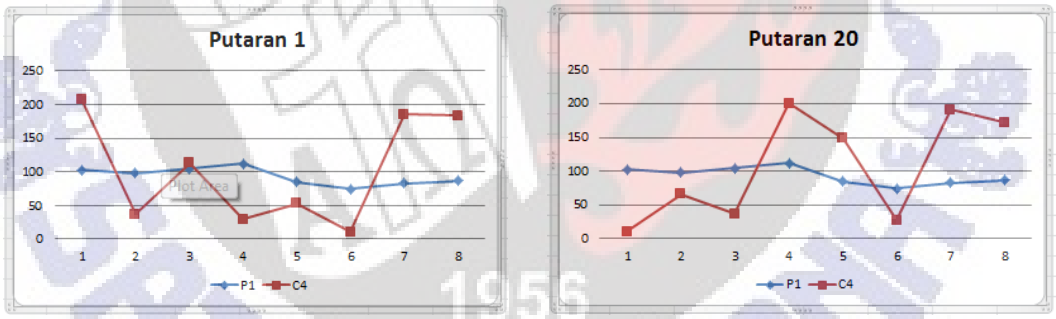
Tabel 6 merupakan hasil uji AE*(Avalanche effect)* pada algoritma kriptografi dengan pola *launchpad* yang dilakukan sebanyak 20 kali. Di dalam tabel terjadi kenaikan dan penurunan di tiap putarannya yang diulang sebanyak 20 kali, pada putaran 20 terjadi hasil rata-rata maksimal dari nilai AE*(Avalanche effect)*. Nilai AE*(Avalanche effect)* sangat dibutuhkan bagi sebuah *block cipher* karena akan menguji seberapa banyak perubahan sebuah bit dan seberapa besar pengaruhnya pada bit *ciphertext*.

Pengujian korelasi digunakan untuk mengukur seberapa acak perbandingan antara hasil enkripsi *(ciphertext)* dan *plaintext*. Nilai korelasi sendiri berkisar 1 sampai -1, dimana jika nilai kolerasi mendekati 1 maka *plaintext* dan *ciphertext* memiliki hubungan yang sangat kuat, tetapi jika mendekati 0 maka *plaintext* dan *ciphertext* memiliki hubungan yang tidak kuat.

Tabel 7 Nilai Korelasi Setiap Putaran

HASIL KOLERASI			
Putaran	**Kolerasi**	**Putaran**	**Kolerasi**
1	0,028384531	**11**	0,440284414
2	-0,595520276	**12**	-0,027764385
3	0,206432613	**13**	0,442312865
4	0,239886698	**14**	0,268721931
5	-0,525061155	**15**	-0,134143603
6	-0,596482531	**16**	0,205903744
7	-0,492724086	**17**	0,028858442
8	-0,849007823	**18**	0,547182013
9	-0,214967294	**19**	0,233288069
10	0,13380066	**20**	-0,053678646

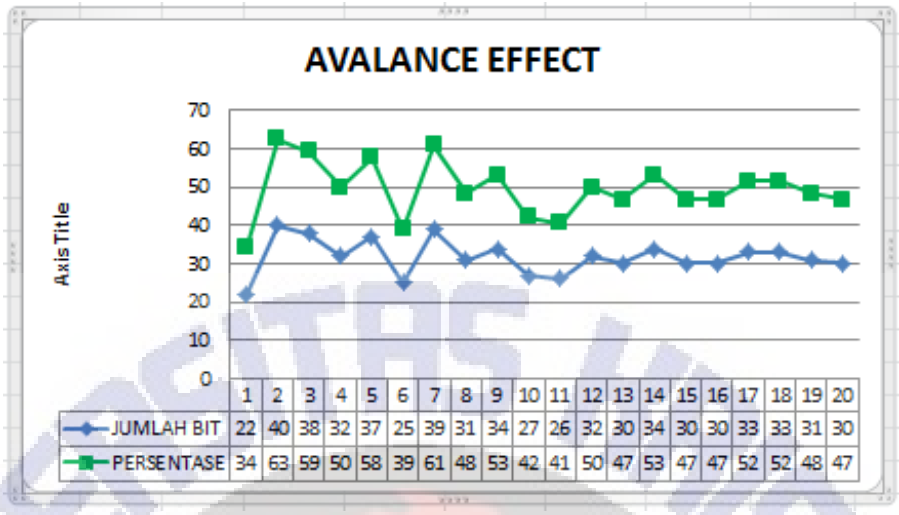
Pada Tabel 7 dari 20 putaran yang di uji setiap putaran memiliki nilai kolerasi lemah sehingga dapat disimpulkan bahwa algoritma berbasis *Block Cipher* 64 bit dengan pola *launchpad the chainsmoker – closer (launchpad pro)-youtube* dapat menghasilkan nilai korelasi enkripsi acak yang dapat dibuat dalam bentuk grafik pada Gambar 14. Korelasi di tiap proses berbeda-beda tetapi memiliki hasil terakhir di -0,053678646 yang digolongkan sangat rendah.



Gambar 14 Grafik Perbandingan *Plaintext* dan *Ciphertext*

Gambar 14 menunjukkan bahwa pada setiap putaran terdapat perbedaan yang signifikan antara bilangan desimal *plaintext* dan bilangan desimal *ciphertext.*

Pengujian AE*(Avalanche Effect)* dilakukan untuk mengetahui seberapa besar perubahan bit ketika karakter *plaintext* dirubah. Pengujian dilakukan dengan 3 (Tiga) contoh *plaintext* dan kunci (*key*) yang berbeda dan kemudian akan diubah 1 (Satu) karakter pada *plaintext* sehingga menghasilkan perbedaan *Avalanche Effect* pada setiap putarannya.



Gambar 15 Grafik Pengujian *Avalanche Effect*

Pada Gambar 15, menunjukkan grafik pengujian AE*(Avalanche Effect)* yang digunakan. Dalam grafik ini menunjukkaan *avalanche effect* yang tidak stabil namun segnifikan pada masing-masing putaran. Dalam grafik ini *plaintext* yang digunakan adalah "gbipUKSW" yang diubah menjadi "GBIPuksw" dengan menggunakan kunci "mAiP2472".

5. Simpulan

Berdasarkan penelitian dan pengujian terhadap perancangan kriptografi *block chiper 64 bit* berbasis pola *launchpad the chainsmoker – closer (launchpad pro)-youtube* dalam 20 putaran enkripsi dan 20 putaran deskripsi memenuhi prinsip dan menghasilkan nilai kolerasi yang sangat rendah antara *plaintext* dan *ciphertext*. Terdapat perubahan segnifikan pada analisis *avalanche effect* karena terdapat kombinasi prinsip-pripsip kriptografi tranposisi, jaringan *feistel* dan substitusi tabel *S-Box* yang terpasang pada setiap proses dan semua putaran. Pada pengujian *avalanche effect* mempunyai rata-rata 49,53125% dan mendapatkan nilai terendah 34,375 dan tertinggi 60,9375. Hasil akhir dari 20 putaran enkripsi -0,053678646 mempunyai nilai rata-rata -0,035714691. Semoga dalam metode perancangan kriptografi ini dapat menghasilkan teknik kriptografi baru dan membantu meningkatkan keamanan data yang mengganggu komunikasi. Tentu saja dalam kemajuan teknologi memberikan banyak keuntungan bagi kehidupan manusia.

6. Daftar Pustaka

[1] Ariyus[1], Dony[1], 2006, *KRIPTOGRAFI Keamanan Data Dan Komunikasi*. Penerbit Graha Ilmu: *Yogyakarta.*

[2] Simarmata, Janner. 2006. Pengamanan Sistem Komputer.Penerbit Andi: Yogyakarta.

[3] M. Backes. (2011). *Block Ciphers* [Online]. Available: http://web.cs.du.edu/~ramki/courses/security/2011Winter/notes/feistelProof.pdf.

[4] Junod, Pascal & Canteaut, Anne (2011). Advanced Linear Cryptanalysis of Block and Stream Ciphers. IOS Press. p. 2. ISBN 9781607508441.

[5] Cusick, Thomas W. & Stanica, Pantelimon (2009). Cryptographic Boolean functions and applications. Academic Press. pp. 158–159. ISBN 9780123748904.

[6] Schneier B., Applied Crytography, Second Edition, John Wiley & Sons, Inc., 1996. Diakses dari http://www.sarjanaku.com/2012/11/pengertian-kriptografi-definisi.html

[7] Thomas Adhi Nugroho, 2015, "Perancangan Algoritma Kriptografi Berbasis Pada Bagian Pohon" Salatiga : Jurusan Teknik Informatika, Universitas Kristen Satya Wacana.

[8] Guntoro, 2016, "Perancangan Kriptografi *Block Cipher* Berbasis Pola Ikan Berenang" Salatiga : Jurusan Teknik Informatika, Universitas Kristen Satya Wacana.

[9] Lyonly Evany Tomasoa, 2016, "Pengaruh *s-box advanced encryption standard (AES)* Terhadap avalanche effect pada Perancangan Kriptografi *Block Cipher* 256 Bit Berbasis Pola Teknik Tarian Dansa Tali Dari Maluku" Salatiga : Jurusan Teknik Informatika, Universitas Kristen Satya Wacana.

[10] Fitri Maak, 2006, "*Cipher* Blok (*Block Cipher*)". Diakses dari http://www.academia.edu/7253321/Cipher_Blok_Block_Cipher

[11] Munir, Rinaldi. Bahan Kuliah IF5054 Kriptografi. (2004). Departemen Teknik Informatika, Institut Teknologi Bandung.